



RUNAS RADIO



<http://www.runasradio.com>



Richard
Campbell

RunAs Radio is a weekly Internet Audio Talk Show for IT Professionals working with Microsoft products. The full range of IT topics is covered from a Microsoft-centric viewpoint.



Greg
Hughes

Text Transcript of Show #083
(Transcription services provided by [PWOP Productions](#))



Chris Stoneff Fixes Our Passwords!
November 12, 2008



[Music]

Brandon Wenn: From runasradio.com, you're listening to RunAs Radio, the Internet audio talk show for IT professionals with Richard Campbell and Greg Hughes. This is Brandon Wenn, announcing show #83, with guest Chris Stoneff, recorded Thursday, October 23, 2008. RunAs Radio is produced each week by PWOP Productions, providing professional media and podcasting services online at pwop.com.

Richard Campbell: You're listening to RunAs Radio. I'm your host, Richard Campbell, and with me as always my co-host, Greg Hughes.

Greg Hughes: Howdy. How is it going?

Richard Campbell Things are good, man. I guess we're off to the next show wherever that may be. I lose track with this whole time shifting of recording thing.

Greg Hughes: Well, see, this is the magic of I'm actually on an airplane flying to Las Vegas right now.

Richard Campbell: You think so?

Greg Hughes: You're in Las Vegas, yet somehow we're able to talk to each other.

Richard Campbell: I don't know how you keep track of all this, but yeah, we're probably in DevConnections and I know we're going to interview Mark Minasi there so that will be good fun.

Greg Hughes: Right, live in front of an audience.

Richard Campbell: There's something about Mark, I think he just sets us off that we all get a little unruly when we start talking.

Greg Hughes: Mark is always an interesting conversation and a whole lot of fun.

Richard Campbell: Yeah, it's good fun.

Greg Hughes: Yeah, and always a good source of information as well, but always a lot of fun to talk to.

Richard Campbell: Well, and it seems like this whole fall, we're going to be doing mostly live shows in front of audiences or recording at conferences so you never know exactly what you're going to get. It's as much fun for us as it is for the listener. For the listener, if you have any questions, concerns, shows we're missing, things you'd like to see us do, send us an email, info@runasradio.com.

Greg Hughes: Right, it's your ideas that drive the content here. We want to make sure we're delivering what you need.

Richard Campbell: Absolutely. All right, let's introduce our guest. Chris Stoneff oversees Lieberman Software's product management and is responsible for integrating the real-world needs of clients into the company's product offerings. With more than 13 years of systems administration, consulting, training and product management experience, Mr. Stoneff is instrumental in guiding the development of the Lieberman Software solutions portfolio. An accomplished consultant and technical trainer, he has taught thousands of administrators on fundamental and advanced concepts of Windows management and security concepts and key technologies. Chris holds more than a dozen certifications including MCSA: Messaging, MCSE: Security, MCT, and CTT+. He is also a frequent contributor to IT publications. Mr. Stoneff has been with Lieberman Software since 2004. Welcome Chris.

Greg Hughes: Hey Chris.

Chris Stoneff: Hey, good to be here. Thank you.

Greg Hughes: It's good to talk to you.

Richard Campbell: So, the topic of the day, Lieberman Software does a bunch of different products but the Password Management Tools are interesting to me. We've never really spent a half-hour on passwords and I think we ought to.

Chris Stoneff: Well, I'd tell you, the passwords are kind of a pain for everybody, for the users, for administrators, and certainly for anything relating to security and this is really where the strength of our product starts to come through.

Greg Hughes: So, let's talk about passwords. Before we dive into maybe solutions for passwords, maybe we should talk about what some of the problems are.

Chris Stoneff: Sure.

Greg Hughes: I know coming from an online banking background, I've had to deal with the fact that passwords are, in many cases, no longer even acceptable at least as the standalone form of authentication but even then, you know, why are passwords are such a weak way of doing things? What are the problems associated with passwords?



Chris Stoneff: Well, the problems associated with passwords are ironically they're the problems where some people, they flat out forget the passwords in the case of the end user or in the case of an account that's been running services for years and nobody knows what's going on, problems are extending for passwords are also revolving around people who know too much because those same passwords have been used for years, and then you have problems where the administrators leave or people start talking and now everybody has access to things that they shouldn't have access to if this password have never been changed.

Greg Hughes: Sharing a single account and password around, that kind of stuff?

Chris Stoneff: Yeah, absolutely. So when you deal with passwords all day long, in and out, there comes a time where you have to change these passwords for these very reasons, you know, unlike things that changed on a regular basis like say Smart Tokens and CatCards and things like that that provides certificate-based forms of authentication that are potentially more secure in any case, there are still some things that require passwords like service accounts where you don't have this interactive log-ins where somebody can punch-in that code or even come by with a card or things like that. So, you're not going to get away with passwords, at least not yet. So, administrators have to deal with them, banks have to deal with them, the government has to deal with them. They're not going anywhere, not for a while.

Greg Hughes: One of the problems of password management has to do with so you take a classic sort of a Windows or any kind of a directory where you can have a policy that the password has to be changed every X number of days. The cost associated with an IT helpdesk or a service desk that has to take calls from users whose accounts have expired, for example, the passwords have expired and they could no longer access their account and they can't do work. Have you had to deal with those kinds of problems? Have you had to think about solutions for that particular problem?

Chris Stoneff: For the end users, most definitely. We have products out there that do allow users to self-serve their own passwords to remove the helpdesk out of the loop and provide full logging of everything that's going on, but when you have users calling up all day every day, helpdesk is busy resetting passwords instead of solving real problems so that's a waste of time and money. Users are spending time to chatting and they're wasting more time beyond just resetting their own passwords so, you know, you got to keep in mind when you set a password policy too, that there's a fine balance

between the type of users that you have to deal with and the type of information that you're trying to protect by having this regular password changes. Certainly end users represent one full stream and there's a lot of companies, they're moving in the direction of managing users passwords and removing, but more to the point what's good with what the companies are doing now, like take Microsoft's UAC for example, these are the same sort of things that OS X is already doing or that UNIX has been doing this for years where they're removing user's rights from being administrators, full-time administrators. In this case, when they let their passwords out, they usually let their passwords out or they forget their passwords and things like that, that's not as big of a deal as it used to be just because they're not necessarily administrators anymore.

Greg Hughes: Right. So the access associated with an account is being limited as opposed to being give them everything as to give them nothing unless you specifically authorized access to certain information. Talking about expiration of passwords, it's great there are tools and there are products out there to help solve problems associated with user account passwords or, you know, whether service accounts or what have you, but you mentioned policy, setting policy, one of the things -- I'll toss an example out there, usability of a policy, I would set a password expression policy as a multiple of 7 so like 42 days instead of 45 days or 60 days so that that way if I change my password on a Tuesday, I'm going to have to change my password again on a Tuesday as opposed to over a weekend where I have to call Helpdesk. Can you think of any other -- are there other recommendations that you generally make as far as policy management goes?

Chris Stoneff: Well, just the fundamental point there is you have to make sure that these passwords are expiring and they're not being circumvented with that simple little password never expires log on an individual account. These are things that all companies have the ability to set and a lot of them do set from time-to-time. As far as good policy, I'm definitely a fan of locking out accounts that failed to log in. I'm definitely a fan of frequent password changes when possible. I mean even just beyond regular user accounts, we have processes in play that change certain account passwords every single day. The problem with long standing accounts is, of course, all that people really need to break into an account is time.

Greg Hughes: Right.

Chris Stoneff: There's no truly definitively secure process, it just takes time so really the best that you can do with security, at least in my opinion, in my experiences, is to make security difficult enough to



bypass where people either give up because the things are changing before they can actually break what they found or to make it so that it takes them long enough where you can actually catch them in the act. So, with regards to specific policies, I would just say frequent, frequent, frequent.

Richard Campbell: Isn't daily a little extreme? Are users going to tolerate that?

Chris Stoneff: I'm sorry, I should explain. Those aren't policies for specific end user. Those are policies that we employ for specific accounts. The things that protect our proprietary data, the items that reside over information that falls under mutual nondisclosure agreement that we have with our partner companies and things like that.

Greg Hughes: All right, so not accounts that end users would typically log into on a regular basis but maybe just an occasional used account type of thing?

Chris Stoneff: Yes, absolutely.

Greg Hughes: Even if you are changing passwords once a day, how do you manage that? I mean how do you make that account usable when you do need to use it?

Chris Stoneff: Well, this gets into some of what we do with our privilege password management or privilege user password management or shared account password management. There are 14 different buzz words I'm sure for how we describe what it is that we're talking about but we provide a number of automated solutions and there are other companies out there that do as well, that set up policies, that will go out and find these accounts and literally change their passwords, in some cases, hourly if you so desire, so you have what is effectively a one-time used password that has a lifetime [unintelligible] you got shoulder surfers or anybody else that might be out there looking at the sticky note that you wrote the 60-character password on to. I said 60 characters. I really was not exaggerating. I mean Windows allows you up to 127 and we can certainly do that as well, but yeah, you need a tool really to do something like that and this gets into what it is that my company offers and what starts to get into our area...

Greg Hughes: Sure. Well, if you're going to change the password more often, if the password interval is shorter than the amount of time it takes for me to write it down on a sticky note, then, you know, that's pretty strong, right?

Chris Stoneff: Well, you know, therein lies the goal not to make it unusable, so presumably if we're

doing 60-character password, we're not giving you a 10-minute lifetime. It's probably going to take you that long to look up and down from what you're writing, but in most cases, the average case is, let's say that you have a password that lives for a day, a 24-hour period that's not so much running special services but is used to access special areas of your network, you know, when you have things that run services, you have to give them a little more leeway because there's a lot of other things that can be affected so you can't change the password every single hour but certainly for those privilege accounts, you have a lot of leeway to do anything that you want to do to make them inaccessible.

Greg Hughes: Right. You are an expert in the industry and everybody has opinions on this but I'd be curious to know what you think about complexity of passwords versus length, especially an interesting conversation always is passwords versus pass phrases. By pass phrase, I mean I might type something like "My dog's name is Skippy" with, you know, natural spacing and punctuation and different things in it but it's long, it's relatively complex. What's your opinion about the right and best way to do things?

Chris Stoneff: The complexity doesn't make so much of a difference at least up to a certain length. Microsoft is my favorite example. They use the LAN Manager Hashes that turn on by default for everything and they apply to all characters or all passwords up to 14 characters unless an administrator has expressly turned off the LAN Manager Hashes and then at that point you only have the NTLM Hashes. The problem with the NTLM Hashes is that 1) Microsoft has been using it since day one, 2) is that there's no salting provided, meaning the hash of the password that you look at today will never vary in any way, shape or form even if you rehash it 10 years from now where if you have something, say, with salt, you hash it once, it looks this way; you hash it again, it looks completely the other way. So, the problem with that is that once you know what the hash algorithm is, which is widely understood, you can literally generate the entire hash population from 1 to 14 characters...

Greg Hughes: As a dictionary, right.

Chris Stoneff: Which again is the length that the Microsoft LM hashes got too and get your password just by comparing hashes. In fact, there are plenty out of tools out there that do that, say, for example, rainbow tables. You can do your search on your favorite search engine, you can download rainbow tables, there are plenty of tools to create them and quite literally, you can go from extracting the LM hashes to comparing them in a rainbow table to obtaining a 14-character mixed case alphanumeric



special character sort of password and get it in less than two minutes.

Greg Hughes: Not necessarily a great scenario for the average administrator, right.

Chris Stoneff: No, not in the least. There are lots of little things that they can do to help out, some of that even comes down to physical security, but when you start dealing -- you know, in that case there you have a 14-character with spaces, with hyphens, with special characters, the pound sign and so on and it doesn't do you a lot of good compared to it might as well just have been a password that said password. Now, if you were to compare that same thing to say something that was 15 characters long, again, using Microsoft as our example, now all of a sudden, you don't have the LM hash. You don't have the widely understood, easily guessable, easily crackable sort of hashes.

Greg Hughes: Right.

Chris Stoneff: So, in that case, even if you did 15 ones in a row, it would be infinitely harder to crack than with, say, something that was my dog Spot that had the zeros and exclamation marks and whatnot. So, definitely, a fan of length over complexity, for sure.

Greg Hughes: Interesting.

Richard Campbell: All right, so what do we mean exactly when we talk about privilege account password management? I know this is a tool that literally makes -- what's a privilege account?

Chris Stoneff: Well, the privilege account we've described as those accounts that have access to, say, privilege areas of your computers and your information. These would be potentially built-in administrators, any of your service accounts which generally you're going to find the majority of your service accounts are going to have some sort of domain Y access to run whatever it is that they're doing on these computers or the scheduled task accounts or the application account.

Richard Campbell: I mean typical administrator account is what we're talking about here.

Chris Stoneff: Okay. So, with your built-in administrator account, these are accounts that exist on every system. In the UNIX world, you refer to this account as route. The account that is always there has the same user ID or relative ID and is therefore easily "enumeratable," if that's even a word, but it means that there's a portion of that ID that we can always look for and save this account, this is the one that we need to focused on breaking on. So, we can

target those accounts quite easily because they have the access to literally the unfettered access and there's nothing you can do about these accounts too.

Richard Campbell: Right.

Chris Stoneff: You know, you can disable them, but in some cases, they'll become re-enabled automatically. Again, Windows is our favorite example. Even if you just disabled the administrator account, it becomes re-enabled the second that you go into safe mode. You can use a Knoppix boot disk to re-enable it, you can use repair process to re-enable it. It's very easy to get back at is what I'm saying. So, when you deal with these accounts, the best that you can do to an administrator is again slow it down by denying it access, by disabling it, but you'll never make it unusable, that's the whole point. So, what we're trying to do with these accounts is limit their attack vectors because, of course, finding the account is one thing but being able to log in as the account is another.

Greg Hughes: Right.

Chris Stoneff: So, what our products are targeting is being able to 1) Identify these accounts no matter what they've been named because, of course, you have to be able to find it in order to manage it and then 2) is change those passwords on a very regular basis because the built-in administrator accounts primarily is that fire call back door, oh my God, I need to fix my system sort of an account at this point.

Greg Hughes: Sure.

Chris Stoneff: And so we want to change those passwords on a regular basis. We want to make sure that nobody knows what the password is, but that we can make them available, the passwords that is, when the accounts are actually needed to perform those disaster recovery type scenarios.

Greg Hughes: So, for the average system administrator who is hearing this information for the first time, this probably sounds a little bit scary.

Chris Stoneff: Well, you know, it can because there are a lot of companies out there that have relied on the build-in administrator to do everything. From simple admin rights, they give their users administrator rights which is a problem in and of itself, but again with that built-in administrator, which is a bigger problem, you have in most cases folks have deployed these computers with scripts, with images, and that means that every computer out there has the same administrator account, has the same password, and in a lot of cases, folks are relying on that from the standpoint of always being able to get into their computers, but from somebody who is trying to break



in, they're relying on that because once they crack one system's password...

Greg Hughes: They've got them all.

Chris Stoneff: They effectively have access to every single system. I mean you got to understand, when you have a domain, you still have individual SAM, the Security Accounts Manager, that's where that built-in administrator resides.

Greg Hughes: Sure.

Chris Stoneff: And all you need to access any of the computers are the username and password. So, when the administrator says, "I'm not comfortable with changing a password," I'm saying how can you be comfortable with leaving it the same for 10 years?

Greg Hughes: Exactly. How can you be comfortable with not changing a password? So, how do we solve that problem? You guys offer tools to help in this area. When you talk about tools, we can talk about process, but how do we solve this problem in a way that's meaningful so that we know that we've got it covered?

Chris Stoneff: You mean with regards to making sure that one computer can access another or do you mean with regards to making sure nobody knows what the passwords are?

Greg Hughes: Yes.

Chris Stoneff: It's all kind of the same thing, but they're all things that administrators need to consider. There are plenty of tools out there. Lieberman Software makes a number of tools that can help them out with these things, but you're looking at, again, regular password changes, you're looking at making sure that when those passwords are transmitted across the network or stored, that they're not sent in plain text. You're looking at making sure that when those passwords are stored, that they're not stored in a safe where you have no idea who is accessing them and when and where and you need to make sure that when people do need access to those passwords, that they can actually get them in a meaningful way meaning where we're actually logging who is gaining access, when they're gaining access, and what they're doing with these things for. So, like you said, my company certainly makes a number of tools but there are other people out there too that make tools for this as well.

Greg Hughes: Right. You need to be able to have an audit trail so that we can see who did what.

Chris Stoneff: Right. Well, if they have to deal with anything like SOX or PCI or just basic company governance...

Greg Hughes: Right.

Chris Stoneff: Knowing who has access to the administrative account when, where, and how is absolutely mandatory and when you're in that baseline scenario where you have every single computer deployed with the same account and the same password and you've had administrators come and go, you've had helpdesk come and go, you really have no idea who is actually causing a problem using these built-in accounts.

Greg Hughes: I appreciate the fact that you work for a company that build software to help solve these problems and I appreciate the fact that I have to push you a little bit to talk about what you guys have done, but why don't you tell us what you guys have done specifically to help administrators in enterprises or companies solve this problem with your tools. What do you enable? What do you do that's above and beyond the tools they get just with the Windows or the Active Directory infrastructure that they buy?

Chris Stoneff: Well, you know, it's funny. Windows doesn't provide you with a single thing to manage all of your systems at once. They give you the Computer Management Interface or the Active Directory services to do, in the case of Active Directory, you can do the domain built-in administrator, and in the case of Computer Management, you can do that single computer's administrator but that's relying on human touch and it's not addressing the needs of logging, the needs of secure access, or anything like that. So, what our tools do, there are a couple of different tools that we can do but we're focused on one in particular called Enterprise Random Password Manager or ERPM as what we refer to it from here. What it does is it allows you to do on this automated basis and that's really the key is to identify all of your systems that are out there and it does this automatically and builds the system to support you because obviously if you don't know what's out there, then you're not managing everything and that's really one of the key components to ensuring your security as in ensuring that you know that you're managing everything.

Greg Hughes: Sure.

Chris Stoneff: So, one, once we get to the systems, then what this Enterprise Random Password Manager does is it allows you to create a password change op for a scheduled basis that will go out and touch every single system and purposefully break that peer-to-peer model by giving each and every single computer, if we're talking about the built-in



administrator account as an example, by giving each and every one of those accounts a totally unique password up to 127 characters if you want, but in any case, so when you give every single computer that totally unique password, you're fixing the problem number one of the fact that by breaking one computer, you're effectively a domain administrator because now you have the password to every single system, you're fixing that problem because no two machines have the same password. So, if by chance you break one, it's just the one system so you're limiting the scope of their attack. Two, with the scheduled basis, we can do this very frequently as much as hourly, as often as yearly if they see fit. So, by doing again the automated changes, there are a couple of things that's happening there as we're doing regular changes because, again, as we have mentioned before, all people need is time to get into a system so if we change it regularly, you're limiting that time and attack vector so that's a good thing. Three, because it's automated and done by the tool, nobody knows what the passwords are, not right away. We're going to provide them access to it in a delegated and audited fashion in our web interface, but until that time, nobody knows what the password is so think about it from a company standpoint or from that IT administrator standpoint. We just fired junior admin or we just fired head admin or head admin left for whatever reason, maybe it wasn't such a good breaking of ties here, but without a tool like this, we need to worry about what systems you can get into and what his attack vectors are.

Greg Hughes: Sure.

Chris Stoneff: Well, if you can eliminate that hole that exists on every single system, you've really mitigated his ability to cause a lot of damage, and now you're just back at two other real attack vectors for him in terms of using accounts and the passwords is the service accounts and would be his own account. Well, disabling his own account is one thing. That's very easy. That's just right click, disable.

Greg Hughes: Service account is a whole different story.

Chris Stoneff: Right because you've got to build an admin account of course for managing and providing access to when people need it but until then nobody knows it, but you still have that privilege process account. That's the one that's really scary to administrators. For many reasons, from simple stuff to, you know, I don't want to take down my business to change this password but I know I have to, to we have no idea where this account is actually used in our environment. We like to think that it's used for, let's take our average company here, we would like to believe it's used for just these 10,000 or 15,000 servers but in reality, I know that it could be used on

services that weren't documented on some of these servers, I know that it could be used to run services on my workstations because my developers or my other administrators were doing things with these accounts and they have to go through a change process to get a new service account. So, they don't do that. Instead they just use an account that they already know because again you're looking at accounts that will rarely change and not for a good reason but for fear.

Richard Campbell: Yeah, fear of breaking things.

Chris Stoneff: Right, fear breaking things, absolutely. I mean if you consider, if you take the average failure rate or misrate, let's say it's even 1% of 10,000 computers, it's still a hundred systems.

Richard Campbell: Yeah.

Chris Stoneff: I'm doing math right. That's still a lot of systems that are going to fail right off the batch just because we missed that password. Now, if you figure generic lockout account policies, say, three times within a period of time and we're going to lock up the account, well, now, missing that 1% of your systems has killed that service account...

Richard Campbell: Right.

Chris Stoneff: And everything that depends on that service account is going to fail. Now, if you talk about these are the databases that house our transactions, for our company when we're doing purchasing or we're doing sales, or anything like that, or maybe it's the back-up strategy for people's payroll, you know, there's a lot of horrible, horrible things that can happen and you're talking literally billions of dollars because of even an hour of downtime in some cases to fix this, let alone even trying to track it down. So, again, dealing with that Enterprise Random Password Manager, the scope extends beyond just changing the built-in admin account password that extends into these process accounts and process, I mean including service and task and application and so on.

Greg Hughes: Right.

Chris Stoneff: So when we go to change these process accounts on a regular basis, and this isn't something that you should be doing -- you should be doing it often but you can't do it as often as you can, say, a built-in administrator just because, again, of the scope of what these accounts can affect. So, when we change these process accounts with Enterprise Random Password Manager, it's the same thing as Automatic System Discovery, create the password policy change job and when we go through and we change these accounts, it's that we're also



scanning on each of our target systems the services, the scheduled tasks, the COM objects, the applications, all of these things that exist on these machines, we are scanning to make sure that when we change this process account that we are also getting everywhere with this account as reference.

Greg Hughes: Got you.

Chris Stoneff: Now you got to consider what that means, the scope of this.

Richard Campbell: That's a lot.

Chris Stoneff: Everywhere where that accounts is referenced, right? Again, we're talking about trying to remove that fear, that fear of what happens when I change an account so we can give them kind of a read-only view where they can see beforehand what's out there and its interesting even in our own environment sometimes how I find users using their own accounts for services on their own systems or for scheduled tasks and they wonder why their account gets locked out. All our tools gave us that view to see, "Okay, how did you get yourself locked out if you didn't type in your password wrong?" "Well, they just change it."

Greg Hughes: Right.

Chris Stoneff: You know, we just updated the Active Directory portion but...

Greg Hughes: But the scheduled task is still running under the old password, yeah.

Chris Stoneff: Right and again this is what our Enterprise Random Password Manager tool is solving for those process accounts, for those built-in admin by automatically developing that list of services and things of that nature of how the account is used. When we randomize the password for this account, we probably gave that random password to everyone where that account is used which means that the likelihood, because of this discovery of you having a network outage, is greatly minimized.

Greg Hughes: One of the difficulties with putting strong IT controls in place is that quite often it does requires so much high touch people time so applications like yours and others that enable automation and discovery of information really help those people to touch the next layer of work if you will so they could be used in a more service-oriented or smarter kinds of ways as opposed to trying to discover things and solve problems, prevent the problems in the first place and let those people actually interact with users or solve problems.

Chris Stoneff: Absolutely. One of the things that some of our customers have told us about how they managed services in the past range from the most obvious which is we don't manage those accounts because we don't know how they're used to we have a month set aside, a whole month set aside every year where we hire in these contractors which are the folks making \$10 an hour to come in and change this and then we deal with the failure rate after the fact, and then we have our customers who say, "Well, we just use your tool." Even though I'm not allowed to fully automate the process, I don't have to involve a whole team, you know, I can sit here on a late Friday night and do the change and see the failures as they occur for whatever reason because the system wasn't sane or I can say, "Oh, that's not a real problem because it doesn't actually affect anything else," and I can go on with life and only involve myself and not 20 other people so I'm saving the company money by doing that and I'm saving everybody time and in fact saving my time because I can do this on a single night and then the people who are allowed to do a fully automated go, it's great. I let your tool run and it takes care of any errors that occur all by itself.

Greg Hughes: Right. Well, not only are you saving money and time, you're also, while saving money and time, creating a more secure environment.

Chris Stoneff: Right, absolutely and then the nice side effect of all that is because everything is logged from everything that the tools do through all the password recoveries and whatnot because all of that is logged and available on reports and accessible to the authors. We're also ensuring that these companies don't have problems with their own internal or external auditors. Think again of SOX or PCI compliancy were often these companies make sure they don't get blacklisted. We're literally giving them air to breathe.

Greg Hughes: Right and ultimately, if you're not getting blacklisted, if your auditors are happy, that's a side effect of a strong, well-controlled and healthy environment which really should be the ultimate goal, not just making auditors happy but having auditors be happy as a side effect of just doing things really well.

Chris Stoneff: Absolutely correct.

Richard Campbell: Gentlemen, I think we're just about out of time. Chris, can you walk me through one thing on this which is walk me through the process of getting a password back now. I know it's changed all the time. I need to log in as an administrator. What does it look like to go get a password?



Chris Stoneff: Okay. Well, with the Enterprise Random Password Manager, what it looks like is you go to this secured web interface, you'll input your Active Directory credentials. We're not maintaining duplicate accounts databases, one for us, one for them. So, you log in and then through the rights that have been delegated to you, you will only be able to see certain systems and even certain accounts and then from there, you'll choose the account on the system that you've been delegated the rights to access, log of course your login and this request, and then depending on how things are set up, you'll leave a generated request which will be approved or denied for that password or you'll simply be able to recover that password. Either way, it's going to generate an email of that recovery and that at that point you'll get your password which, hopefully, is at least 15 characters long and then if you sit there on that page for a period of time, that page will automatically navigate you ways to help circumvent shoulder surfers, you know, those people watching everything that you're doing. You're going to take that password, which is going to be valid for a period of time and do your work. Now, whatever that work is, if you haven't extended that checkout, and by check-out I mean only you have it, nobody else can get that password at that point and time unless you're the one expressly giving it to them, now if you haven't check-in that password by the end of that lifetime of the password, then the password is going to automatically re-randomize because maybe you went home, maybe you're out to lunch, hard to say, but the password will forcibly re-randomize after a period of time unless you've extended the check-out. Now, if you're done, you go in, all you have to do is restore the image at the machine, rejoin it to the domain as that built-in administrator. Now you're done and you don't need the password anymore and you want to make sure that you're not responsible, then you can come right back into that web interface and click that check-in button which is going to help insure that 1) the password will be re-randomized immediately, 2) there's a log that you were done with password which is also indicative of the fact that the password was re-randomized and of course we're going to log that check in as well so we know when he did it, where he did it, how you did it.

Richard Campbell: Cool.

Greg Hughes: Did I hear you say that it sounded like that maybe there was an option in there for some kind of a secondary approval before the password is given to somebody?

Chris Stoneff: Yes, absolutely correct. We want people to get passwords when they should have it and in some cases, you know, it's as simple as just coming in and saying recover, but in other cases, it's not just guaranteed that they should have access to a

password so we do have a Workflow process in there where folks can go through a request and certain people are allowed to either grant or deny that request for the password.

Greg Hughes: I can think of several situations where that would be useful especially in a SOX environment like access to finance database management account, for example, that type of thing.

Chris Stoneff: Sure, sure.

Greg Hughes: You want to be able to document an approval.

Chris Stoneff: We can even do you one better too as that in the web interface, there's also an option to remote desktop to the target system, not that it's necessarily offline, just that we need that built-in admin or fire call account to get into the system to fix whatever the problem is without ever displaying the password to the end user. We can create an RDP session to the systems and automatically log them in with those administrator rights to do whatever they need to do.

Greg Hughes: And handle that as a one-time password event and then change it as soon as it's done.

Richard Campbell: All right, gentlemen, we've had a good security geek out. I guess we were due and certainly some great insight into thinking about passwords at enterprise level. Thanks so much for coming on the show, Chris.

Greg Hughes: Thanks Chris.

Chris Stoneff: Thank you very much for having me.

Richard Campbell: And we'll talk to you next week on RunAs Radio.